

Quantum Computations and Unitary Matrix Decompositions

Stephen S. Bullock

Mathematical and Computational Sciences Division
Information Technology Lab
National Institute of Standards and Technology

Outline

- I. Quantum Data and Quantum Computation
- II. Quantum Circuits Using QR and Cosine-Sine
- III. Two-qubit Circuits and the Canonical Decomposition
- IV. On-Going Work (Generalized Canonical Decompositions)

Quantum Computing

- replace bit with qubit: two state quantum system, states $|0\rangle, |1\rangle$
- quantum data states obey axioms of quantum mechanics
 - Single qubit state space $\mathcal{H}_1 = \mathbb{C}|0\rangle \oplus \mathbb{C}|1\rangle \cong \mathbb{C}^2$
 - $|\psi\rangle = |0\rangle + i|1\rangle$
 - n -qubit state space $\mathcal{H}_n = \bigotimes_1^n \mathcal{H}_1 = \bigoplus_{\bar{b}} \text{an } n \text{ bit string } \mathbb{C}|\bar{b}\rangle \cong \mathbb{C}^{2^n}$
 - two-qubit example: $|\psi\rangle = |00\rangle + |11\rangle$
 - * Both qubits in same state; equal chance of 0, 1

Quantum Computing Cont.

- density matrix ρ : Hermitian matrix describing stochastic dispersion of pure states $|\psi\rangle$
 - Choice of diagonalizations specifies mixture
 - For $\vec{x} = |\psi\rangle$ pure, unmixed density matrix is $\rho = |\psi\rangle\langle\psi| = x\bar{x}^t = xx^*$
 - All states **pure** for rest of talk
- **quantum computations**: apply $2^n \times 2^n$ **unitary matrix** u to n -qubit data strings, i.e. $\vec{x} \mapsto u\vec{x}$

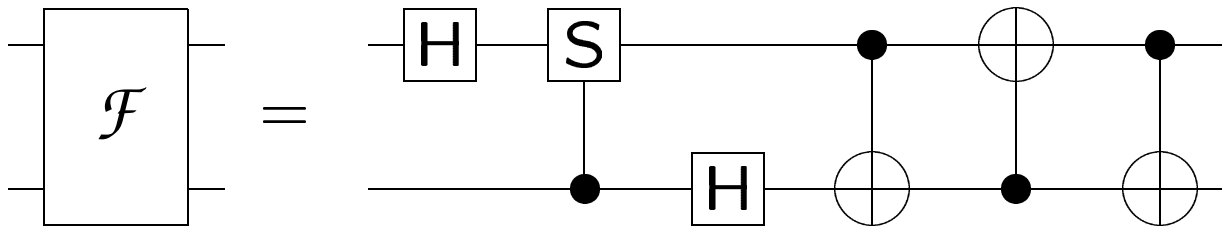
Thm: ('93, Bernstein-Vazirani) The Deutsch-Jozsa algorithm proves quantum computers would **violate the Church-Turing hypothesis**.

Example: \mathcal{F} the Two-Qubit Fourier Transform in $\mathbb{Z}/4\mathbb{Z}$

- Relabelling $|00\rangle, \dots, |11\rangle$ as $|0\rangle, \dots, |3\rangle$, the **discrete Fourier transform** \mathcal{F} :

$$|j\rangle \xrightarrow{\mathcal{F}} \frac{1}{2} \sum_{k=0}^3 (\sqrt{-1})^{jk} |k\rangle \quad \text{or} \quad \mathcal{F} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

- one-qubit unitaries: $H = (1/\sqrt{2}) \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $S = (1/\sqrt{2}) \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$



Tensor (Kronecker) Products of Data, Computations

- $|\phi\rangle = |0\rangle + i|1\rangle$, $|\psi\rangle = |0\rangle - |1\rangle \in \mathcal{H}_1$
 - interpret $|10\rangle = |1\rangle \otimes |0\rangle$ etc.
 - composite state in \mathcal{H}_2 : $|\phi\rangle \otimes |\psi\rangle = |00\rangle - |01\rangle + i|10\rangle - i|11\rangle$
- Most two-qubit states are **not** tensors of one-qubit states.
- If $A = \begin{pmatrix} \alpha & -\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix}$ is one-qubit, B one-qubit, then the two-qubit tensor $A \otimes B$ is $(A \otimes B) = \begin{pmatrix} \alpha B & -\beta B \\ \bar{\beta} B & \bar{\alpha} B \end{pmatrix}$. Most 4×4 unitary u are **not** local.

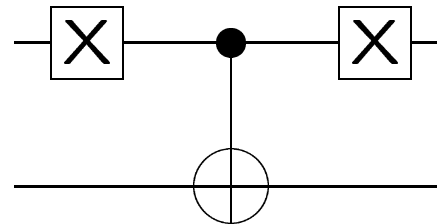
Quantum Circuits

- Quantum computation **complexity** \sim size of quantum circuit
- Typical choices of gates
 - Any two-qubit
 - one-qubit, and **CNOTs** ($|b_1 b_2\rangle \mapsto |b_1(b_1 \oplus b_2)\rangle$), ($|b_1 b_2\rangle \mapsto |(b_1 \oplus b_2)b_2\rangle$)

Quantum Circuits Cont.

- For $X = \text{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, sample quantum circuit:

$$u = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ is implemented by}$$



- good quantum circuit design: find **tensor factors** of computation u

Outline

- I. Quantum Data and Quantum Computation
- II. Quantum Circuits Using QR and Cosine-Sine
- III. Two-qubit Circuits and the Canonical Decomposition
- IV. On-Going Work (Generalized Canonical Decompositions)

Circuit Synthesis by QR Decomposition

- universality argument(1995): circuits for **arbitrary** u
- observation (2000): argument implements **QR decomposition**
 - In general, $m = qr$, with q unitary, r upper-triangular
 - q is made of Givens rotations
 - m unitary demands $r = q^*m$ unitary, i.e. r diagonal
- two-qubit **Givens rotation**: $G_{10,11}$ acts on $|10\rangle$ and $|11\rangle$ by 2×2 matrix v

$$G_{10,11} = \begin{array}{c} \text{---} \bullet \text{---} \\ | \\ \text{---} \boxed{v} \text{---} \end{array} = \begin{pmatrix} \mathbf{1} & 0 \\ 0 & v \end{pmatrix}$$

QR reduction of 4×4 unitary

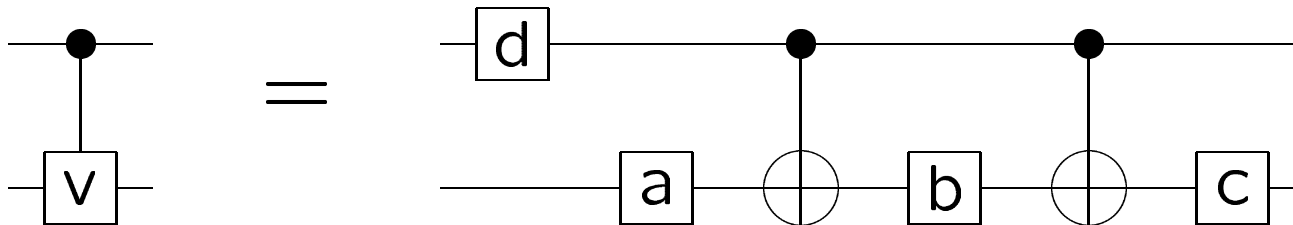
$$\begin{pmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{pmatrix} \xrightarrow{G_{10,11}} \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ 0 & * & * & * \end{pmatrix} \xrightarrow{G_{01,10}}$$

$$\begin{pmatrix} * & * & * & * \\ * & * & * & * \\ 0 & * & * & * \\ 0 & * & * & * \end{pmatrix} \xrightarrow{G_{10,11}} \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ 0 & * & * & * \\ 0 & 0 & * & * \end{pmatrix} \xrightarrow{G_{00,01}}$$

$$\begin{pmatrix} * & * & * & * \\ 0 & * & * & * \\ 0 & * & * & * \\ 0 & 0 & * & * \end{pmatrix} \xrightarrow{G_{10,11} \circ G_{01,10}} \begin{pmatrix} * & * & * & * \\ 0 & * & * & * \\ 0 & 0 & * & * \\ 0 & 0 & 0 & * \end{pmatrix}$$

Circuits for Givens Rotations

- Barenco et al.: $G_{10,11} = 2$ CNOTs + 4 (variable) one-qubit gates



– a, b, c and d are computed from v

- Givens rotation $G_{01,10}$ on $|00\rangle, |01\rangle$ is the conjugation of $G_{10,11}$ by $X \otimes 1$

$$G_{00,01} = (X \otimes \mathbf{1})(\text{topC-}v)(X \otimes \mathbf{1}) = \begin{pmatrix} v & 0 \\ 0 & \mathbf{1} \end{pmatrix}$$

Summary of *QR* Circuit Synthesis

- **Breakthrough:** Every unitary u possesses a quantum circuit.
- Roughly, Givens rotations build circuit entry by entry.
- This design philosophy often ignores underlying structure.
- General philosophy recurs in circuit design:
 - Choose matrix decomposition
 - Produce circuits factorwise

Cosine-Sine Decomposition

Cosine-Sine Decomposition factors a $2^n \times 2^n$ unitary u :

$$u = \begin{pmatrix} v_1 & 0 \\ 0 & v_2 \end{pmatrix} \begin{pmatrix} c & s \\ -s & c \end{pmatrix} \begin{pmatrix} v_3 & 0 \\ 0 & v_4 \end{pmatrix}$$

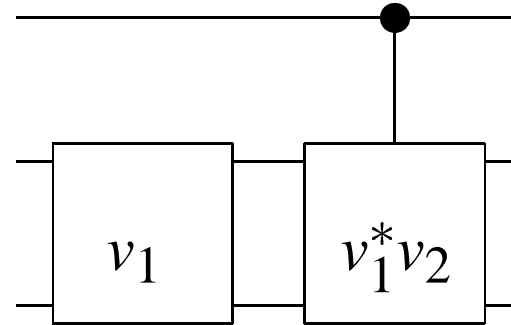
- v_1, v_2, v_3, v_4 are $(2^n/2) \times (2^n/2)$ unitary
- $c = \text{diagonal}(\cos t_0, \cos t_1, \dots, \cos t_{2^n/2-1})$
- $s = \text{diagonal}(\sin t_0, \sin t_1, \dots, \sin t_{2^n/2-1})$

Remark: Decomposition of unitary matrix, not arbitrary matrix

More structure?

Cosine-Sine Decomposition Cont.

$$\begin{pmatrix} v_1 & 0 \\ 0 & v_2 \end{pmatrix} = \begin{pmatrix} v_1 & 0 \\ 0 & v_1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & v_1^* v_2 \end{pmatrix} =$$



- Side matrices of **C.S.D.** do not change top qubit
- Good choice (?) when measurement of single qubit is output
- [q-ph/0303039](#) (B-,Markov): Circuit for cosine-sine matrix

Outline

- I. Quantum Data and Quantum Computation
- II. Quantum Circuits Using QR and Cosine-Sine
- III. Two-qubit Circuits and the Canonical Decomposition
- IV. On-Going Work (Generalized Canonical Decompositions)

The Magic Basis of Two-Qubit State Space

- The **magic basis** of phase shifted Bell states is

$$\begin{cases} |m1\rangle &= (|00\rangle + |11\rangle)/\sqrt{2} \\ |m2\rangle &= (i|00\rangle - i|11\rangle)/\sqrt{2} \\ |m3\rangle &= (i|01\rangle + i|10\rangle)/\sqrt{2} \\ |m4\rangle &= (|01\rangle - |10\rangle)/\sqrt{2} \end{cases}$$

These are maximally-entangled states. Global phases are important.

Theorem (Lewenstein, Kraus, Horodecki, Cirac 2001)

Consider a two-qubit computation U with $\det(U) = 1$

- Compute matrix elements in the magic basis
- (All matrix elements are real) $\iff (U = A \otimes B)$

The Two-Bit Entangler

- **Entangler unitary E** takes computational basis to the magic basis:
 $|00\rangle \mapsto |m1\rangle, |01\rangle \mapsto |m2\rangle, |10\rangle \mapsto |m3\rangle, |11\rangle \mapsto |m4\rangle$

$$E = \frac{\sqrt{2}}{2} \begin{pmatrix} 1 & i & 0 & 0 \\ 0 & 0 & i & 1 \\ 0 & 0 & i & -1 \\ 1 & -i & 0 & 0 \end{pmatrix}$$

Corollary Consider u 4×4 unitary, $\det u = 1$. Then

$$(u = A \otimes B) \iff (EuE^* \text{ is real orthogonal})$$

An Example of the Isomorphism

We choose some orthogonal u , $\det(u) = 1$.

$$u = \frac{\sqrt{2}}{2} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}$$

Then EUE^* is a tensor of one-qubit computations:

$$EUE^* = \frac{\sqrt{2}}{2} \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} = \frac{\sqrt{2}}{2} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \otimes \mathbf{1}$$

Column by column, this amounts to application of the magic basis.

Two-Qubit Canonical Decomposition

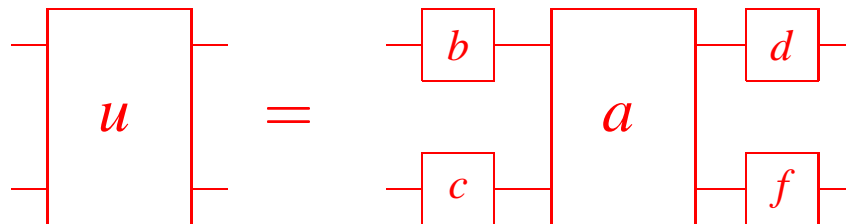
Two-Qubit Canonical Decomposition: Any u a four by four unitary admits a matrix decomposition of the following form:

$$u = (b \otimes c)a(d \otimes f)$$

for $b \otimes c, d \otimes f$ are tensors of one-qubit computations and $a = EdE^*$ for a diagonal matrix $d = \sum_{j=0}^1 e^{i\theta_j} |j\rangle\langle j|$, $\det d = 1$.

Note that a applies relative phases (complex multiples) to the magic basis.

Circuit diagram: For any u a two-qubit computation, we have:



Applications of the Canonical Decomposition

Two-qubit Circuit Design: [(F.Vatan, Colin Williams), (G.Vidal, C.Dawson), (V.Shende, I.Markov, B-)]

- Choose a universal gate library
- In two-qubits, provably optimal or near optimal circuits
 - Implement $b \otimes c, d \otimes f$ as tensor
 - Choose method for circuit for a

Entanglement Capacities: (J. Zhang, J. Vala, S. Sastry, KB Whaley) Only a block may entangle $|\psi\rangle$; other factors are local.

Quantum Circuit Structure: (V.Shende, B-, I.Markov) Recognize u with particularly simple circuits; produce circuits with special case a

Computing the Canonical Decomposition

Step #1: Compute the **unitary SVD** of v unitary:

$$v = o_1 d o_2, \quad d \text{ diagonal}, \quad o_1, o_2 \text{ real orthogonal}$$

Due to a theorem, this decomposition exists.

Step 1a: Suppose $v = o_1 d o_2$, and label $p = o_1 d o_1^t$. Then $v = p(o_1 o_2)$ and $p = p^t$, p unitary. Moreover, we may **compute** $p^2 = v v^t = o_1 d^2 o_1^t$.

Remark: For $p^2 = a + ib$, $1 = p^2 (p^*)^2 = (a + ib)(a - ib) = (a^2 - b^2) + i(ba - ab)$. Thus the real and imaginary parts of p^2 are real symmetric matrices that commute, hence o_1 exists.

Computing the Canonical Decomposition Cont.

Step 1b: Diagonalize to find d^2 . Write $p = o_1 d o_2^t$, with determinants of o_1 and d both one.

Step 1c: Then $v = (o_1 d o_1^t)(o_1 o_2)$ for $o_2 = o_1^t p^* v$.

Step #2: Canonical decomposition results by translation through entanglers. If $E^* v E = o_1 d o_2$, then

$$v = (E o_1 E^*)(E d E^*)(E o_2 E^*) = (b \otimes c) a (d \otimes f)$$

WARNING! Entanglers do not function properly on inputs with $\det \neq 1$.

Outline

- I. Quantum Data and Quantum Computation
- II. Quantum Circuits Using QR and Cosine-Sine
- III. Two-qubit Circuits and the Canonical Decomposition
- IV. On-Going Work (Generalized Canonical Decompositions)

Entanglement Monotones

- **Entangled $|\psi\rangle$:** any non-local $|\psi\rangle$, i.e. not tensor (Kronecker) product
- **Entanglement monotone:** functions that measure how far away a state $|\psi\rangle$ is from local (full Kronecker product)
- Monotones usually map to $[0, 1]$, must return 0 on local states, may return zero on nonlocal states.
 - only detect certain entanglement types
 - types thought to grow exponentially with n

Concurrence

- **concurrence entanglement monotone:** $-iY = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, with $S = \otimes_1^n (-iY)$ a $2^n \times 2^n$ complex matrix. For $\vec{x} = |\psi\rangle$, we have $C_n(|\psi\rangle) = |\vec{x}^t S \vec{x}|$.
- $S = \otimes_1^n (-iY)$ is antidiagonal, $S^t = S^{-1} = (-1)^n S$
- 4-qubit examples
 - maximal 1 on $|GHZ\rangle = (1/\sqrt{2})(|00\dots 0\rangle + |11\dots 1\rangle)$
 - vanishes on entangled $|W\rangle = (1/4)(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle)$

Concurrence Form

Definition: The **concurrence bilinear form** $C_n : \mathcal{H}_n \times \mathcal{H}_n \rightarrow \mathbb{C}$ is given by $C_n(\vec{x}, \vec{w}) = \vec{x}^T S \vec{w}$.

Remark: So $C_n(\vec{x}) = |C_n(\vec{x}, \vec{x})|$.

2-qubits: $C_2(\vec{x}, \vec{w}) = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \end{pmatrix}$

Generalized Entanglers

4-qubit entangler:

$$E_0 = (1/\sqrt{2}) \begin{pmatrix} 1 & i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & i & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & i & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & i & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & i \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & i \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -i & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & i & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Concurrence Canonical Decomposition

Theorem (B-, Brennen) Let v be a $2^n \times 2^n$ unitary, n even. Then $v = k_1 a k_2$ where the factors have the following properties.

- $k_j = E_0 o_j E_0^*$, where o_j orthogonal, $j = 1, 2$
- $k_j^t S k_j = S$, i.e. $C_n(k\vec{x}, k\vec{w}) = C_n(\vec{x}, \vec{w}) \forall \vec{x}, \vec{w}$ in n -qubit data space \mathcal{H}_n
- For a diagonal d , the central factor $a = E_0 d E_0^*$ applies relative phases to the concurrence-one columns of E_0

Algorithm: Computable in same manner as two-qubit canonical decomposition. Given scaling of matrix sizes, numerical issues arise in ≥ 12 qubits.

Application: Concurrence Capacity

Definition: The **concurrence capacity** of a given n -qubit quantum computation ν is defined by $\kappa(\nu) = \max\{C_n(\nu|\psi\rangle) ; C_n(|\psi\rangle) = 0, \langle\psi|\psi\rangle = 1\}$.

Corollary: Let $u = k_1 a k_2$ be the concurrence canonical decomposition of some $2^n \times 2^n$ unitary u . Then $\kappa(u) = \kappa(a)$.

- Calculation: For $n = 2p$, most a have $\kappa(a) = 1$ as $p \rightarrow \infty$.
- Conclusion: Most large unitaries are arbitrarily entangling with respect to the (single) entanglement monotone C_n .

On-going Work

- Most large u in even qubits carry some $|\psi\rangle$ of concurrence 0 to $u|\psi\rangle$ of concurrence 1.
 - Compute numerical examples?
 - How entangled are such $|\psi\rangle$ with respect to other monotones?
- Do the factors have reasonable quantum circuits?
- Odd n : a decomposition exists, do not know algorithm to compute it.
- Analyze particular u from well-known quantum algorithms

Ongoing Work: Numerical Issues

- Algorithm for $(n = 2p)$ -qubit canonical is similar to $n = 2$
 - Diagonalize commuting real $2^n \times 2^n$ matrices a, b , with same orthogonal matrix o
 - Otherwise several matrix multiplications
 - 60-qubits: can't distinguish 2^{60} eigenvalues with 16 digits
- n -odd: complicated decomposition exists, no algorithm